УДК 004.056

Т. А. Кравчук
Науковий керівник: Ю. В. Баришев

МЕТОДИ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ДЛЯ ПСЕВДОНЕДЕТЕРМІНОВАНИХ ГЕШ-ФУНКЦІЙ

Вінницький національний технічний університет

Анотація

У дослідженні виконано аналіз загальних атак, які базуються на пошуку мультиколізій, та конструкцій гешування для протидії їм. Для деяких розглянутих конструкцій гешування підвищеної стійкості необхідне якісне генерування псевдовипадкових чисел. Досліджено відомі генератори псевдовипадкових чисел та запропоновані нові методи формування послідовностей псевдовипадкових чисел. Розроблена програма, що дозволяє виконувати дослідження статистичних характеристик генераторів.

Ключові слова: *гешування, конструкція гешування, загальні атаки, мультиколізії, генератори псевдовипадкових чисел, псевдовипадкові послідовності.*

Abstract

Generic attacks based on multicollisions search hash constructions are to counteract them are analyzed at the work. Some of hash constructions with increased infeasibility needs a quality pseudo-random number generators. Known pseudo-random number generators were analyzed and new methods are proposed. The program was developed which provides the necessary statistics characteristics research of some generators.

Key words: *hashing, hash constructions, generic attacks, multicollisions, pseudo-random number generators, pseudo-random number sequences.*

Одним з методів захисту інформаційних ресурсів є гешування, що використовується для обчислення контрольної суми з метою перевірки автентичності повідомлень, цифрових підписів, пошуку однакових наборів даних, безпечного зберігання паролів в області пам'яті та ін. [1]

Наразі, окрім атак, що здійснюються на основі криптоаналізу, залишається актуальною проблема захисту від загальних атак, які використовують мультиколізії [2]. Для цього необхідна розробка нових конструкцій гешування, які б мали підвищену стійкість до цих атак. Дослідження в даній галузі виявили, що причиною можливості побудови зловмисником мультиколізій є ітеративність процесу гешування [3]. Відповідно для підвищення стійкості пропонується порушувати цю ітеративність. Одним з таких підходів є псевдонедетерміноване гешування [4].

Для реалізації псевдонедетермінованого гешування необхідні специфічні методи генерування псевдовипадкових чисел, які поміж іншим дозволятимуть генерувати числа у змінних діапазонах значень.

Метою дослідження є підвищення стійкості геш-функцій до загальних атак шляхом дослідження генераторів псевдовипадкових чисел (ГПВЧ).

Серед найвідоміших ГПВЧ лінійний та квадратичний конгруентні, а також на основі чисел Фібоначчі.

Лінійним конгруентним генератором з параметрами (x_0, a, c, M) називається генератор, що створює послідовність псевдовипадкових чисел за допомогою рекурентного співвідношення:

$$x_{i+1} = (ax_i + c) \bmod M, i = 0,1,\ldots$$

Квадратичний конгруентний генератор описується таким рекурентним співвідношенням:

$$x_{i+1} = \left(dx_i^2 + ax_i + c\right) \bmod N, i = 0,1,\ldots$$

Конгруентний генератор, що використовує множення з перенесенням визначається рекурентним співвідношенням:

$$x_{t+1} = (ax_t + c_t) \bmod N, t = 0,1,\ldots,$$

де $c_t = c(x_{t-1}, x_{t-2},\ldots,x_0)$ змінюється на кожній ітерації і залежить від аргументів нелінійно таким

чином: $c_t = \left[\frac{ax_{t-1} + c_{t-1}}{N} \right]$.

Загальний вид рекурентного співвідношення, що описує ГПВЧ за принципом Фібоначчі:

$$x_i = (x_{i-r} \Diamond x_{i-s}) \bmod m,\ i = r, r+1, r+2, \ldots,$$

для початкових значень $x_0, x_1, \ldots, x_{r-1}$, де $r, s \in N, (r > s)$ - параметри генератора; $\Diamond$ - символ бінарної операції [5].

Відомі методи генерування псевдовипадкових чисел не забезпечують виконання вимог щодо високого ступеня нелінійності у залежності *i*-го псевдовипадкового числа від (*i*-1)-го або не забезпечують рівномірність розподілу чисел. Для усунення цього недоліку пропонуються нові підходи генерування псевдовипадкових чисел. Розглянуто властивості псевдовипадкових послідовностей, утворених поєднанням принципів квадратичного конгруентного генератора та використання рекурентного приросту:

$$x_{i+1} = (dx_i^2 + ax_i + c_i) \bmod N, i = 0,1,\ldots;\ c_i = \left[\frac{ax_{i-1} + c_{i-1}}{N} \right].$$

Пропонується спосіб удосконалення ГПВЧ на основі чисел Фібоначчі з використанням наступної формули поточного відхилення:

$$r_i = (r_{i-a} + r_{i-b}) \bmod p,$$

де a і b обрані випадково.

Розроблений ГПВЧ з умовою парності, що описується наступним чином:

$$x_{i+1} = (x_i \Diamond x_{i-1} * x_i \bmod 2 - x_i \Diamond i * (x_i \bmod 2 - 1)) \bmod N.$$

Отже, у даній роботі представлено дослідження властивостей генераторів псевдовипадкових чисел, що використовуються в деяких конструкціях гешування для досягнення псевдонедетермінованості.

Наведені результати роботи розробленої на основі досліджень програми надають необхідну статистику для оцінки характеристик досліджуваних генераторів псевдовипадкових чисел.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1. Ferguson N. Practical Cryptography– 2nd ed.// Ferguson N., Schneier B. //New York: John Wiley & Sons, Inc., – 2003 – 493с.
2. Joux A. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions / Antoine Joux// Lecture Notes in Computer Science. – 2004. – № 3152. – С. 306-316.
3. Лужецький В. А. Конструкції хешування стійкі до мультиколізій / Лужецький В. А., Баришев Ю.В. // Наукові праці ВНТУ. – №1. – 2010. – 8 с.
4. Лужецький В. А. Концепція псевдонедетермінованого хешування / В. А. Лужецький, Ю. В. Баришев // Системи управління, навігації та зв'язку. – №3, 2010. – С. 94-98.
5. Харин Ю.С. Математические и компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич// МН: Новое знание – 2003. – 193 с.

Кравчук Тетяна Андріївна — студентка групи 1БС-13б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: domrenysh@gmail.com.

Баришев Юрій Володимирович — к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Tetiana A. Kravchuk — student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, e-mail: domrenysh@gmail.com;

Yurii V. Baryshev — Ph.D., associated professor of the information protection chair, Vinnytsia National Technical University, Vinnytsia.